ATRC
ARIZONA
TRANSPORTATION
RESEARCH
CENTER

RESEARCH NOTES:

Project 534

June 2008

Digital Signature Feasibility Study

Background

The purpose of study was to assess the advantages and disadvantages of using digital signatures to assist the Department in conducting business. The Department is evaluating the potential of performing more electronic transactions (e.g., electronic bidding, procurement, Motor Vehicle transactions, etc.). Many of the Department's candidate transactions require one or more ink signatures before they can be processed. The basic challenge is that without a means to provide verifiable and binding electronic signage; many transactions become Internet ineligible and cannot become part of the Department's e-service portfolio. E-Government relies on secure communication between two or more trusting parties. Digital signatures may provide the missing component that would allow certain transactions to be performed electronically. They may also provide the desired level of security, privacy and authenticity required for the Department's electronic messages. With the volume of e-commerce and business-to-business transactions increasing, the acceptance of digital signatures may be more a question of when, rather than if.

Approach

The study consisted of four main tasks, which included interviews of ADOT staff whose work processes might be candidates for digital signatures, a literature review that included an in-depth analysis of the legal veracity of digital signatures, a survey of other state departments of transportation organizations to ascertain whether any use digital signature technology, and developing advantages / disadvantages of digital signature use by the department along with a cost analysis of two implementation methods (in-house vs. 3rd party).

Stakeholder Interviews

The first task of the study was to conduct interviews with key ADOT staff members. All of the interviewed staff members were knowledgeable about the technology and are well acquainted with potential uses for the technology. As a result of the interviews, a list of potential candidate transactions was created. The transactions were primarily intra-departmental forms (employee system access request forms, timesheets, project files, training requests, etc.). The most complex transaction involved Engineering documents and plan drawings. Many of the internal forms, referred to as "eForms" by department staff, have already been enabled for electronic approvals through ADOT's Adobe LiveCycle product.

Literature Review

The literature review included documentation from many different sources including: Arizona Statutes, administrative codes, policy documents; Federal government statues, policies, and white papers. Independent research was compiled from documented case studies, vendor products and vendor webinars.

What are digital Signatures

In the simplest usage of digital signatures, a user will sign an electronic document with his/her digital signature and then send the document to another person. The second person can electronically verify that the digital signature is valid and that the document had not been modified after it was signed. The second person will use digital keys, signatures and time stamps to enable "authentication" of electronic documents and assurance of the identity of the signature. The tools needed by both people in this process are provided by a Public Key Infrastructure (PKI) system and a trusted third party certification authority. A PKI system creates and manages digital certificates. It is used to grant, renew and revoke digital certificates for end-users. There are a number of standards for PKI messages; Arizona requires that PKI Systems comply with ANSI x.509 and x.500 standards. In order to verify a signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key (which is always kept private). A trusted third party "Certification Authority" provides this service

Legal Review

A.R.S. § 41-132 provides that an electronic signature "may be used to sign a writing on a document that is filed with or by a state agency, board or commission and the electronic signature has the same force and effect as a written signature." An electronic signature has to be (1) unique to the person using it, (2) capable of reliable verification, and (3) linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

The Arizona Electronic Transactions Act (AETA), A.R.S. § 44-7001, is modeled after the Uniform Electronic Transactions Act ("UETA") and was meant to address concerns regarding the incompatible laws between states and the use of electronic signatures by private parties in business transactions.

Retention Guidelines

According to State and Federal guidelines, documents digitally or electronically signed are generally held to follow the same retention requirements as paper documents. The Electronic Signing Policy created by the Office of the Secretary of State (April, 2002 says the signing process information must be retained for the "legal" life of the most enduring document signed. If that "legal" life is unknown, then for at least 30 years. Specific record retention rule schedules for Arizona State agencies are maintained periodically by the Arizona State Library, Archives and Public Records Agency. The most recent update was created on July 3, 2007 and contains specific guidelines State Agencies must follow for retaining documents related to all agency business functions.

State DOT Surveys

The survey of other state departments of transportation focuses on how other states use digital signatures and their plans to implement the technology in the future. The survey determined which methods have been used to implement the technology and identified which vendors have been used and overall satisfaction with those vendors. Finally, the survey attempted to understand how well other DOTs have achieved the benefits associated with their implementations.

Forty-seven DOTs were contacted and detailed responses were received by thirty-six, which was a 77% response rate. The survey was distributed electronically. Detailed contact information was provided by thirty-three DOTs.

Survey Findings

The use of digital signature technology is gaining traction with other state's DOTs. More than half the respondents have already implemented the technology (55.6%) and another 70.5% expect to do so within the next 2-3 years. For the states not using the technology (44.4% of the respondents), the two most commonly cited reasons for not implementing the technology were: The technology was not considered a priority (50%) and that the technology faced legal and regulatory barriers (22%). Digital signature technology is most commonly used to support internal processes (47%). This is followed by engineering design and bidding process (26%), customer-based processes (19%).

The states that have implemented digital signature technology, have selected using third party software over building customized solutions internally (88.9% use third party software; only 11% have built an internal solution). The respondents are very happy with their vendor selection. Nearly 94% said they would recommend the vendor they used.

The majority of states that have implemented some form of digital signature technology report their programs have met or exceeded their expectations (72%). Because many states have recently implemented their programs, 28% reported it was too early to tell. Not a single respondent believed their programs wouldn't eventually meet expectations.

Legal Findings/ Levels of Trust

Although Arizona and Federal statutes clearly approve the use of electronic and digital signature technology for conducting business, the statutes do not prescribe when an entity should apply full digital signature technology over an electronic signature. The State of Arizona, Policy Authority, Office of Secretary Electronic Signing Policy (April, 2002), provides guidelines that agencies should consider. Agencies must "determine what level of trust (basic, medium, and high) is appropriate for their needs. Applications requiring higher assurance must incorporate a technology approved for those higher levels of trust. Establishing trust levels is based on the potential risk involved and levels of security for the highest risk type of transaction. There are three trust levels:

Basic: "there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious."

Medium: "risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial."

High: "threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk."

According to the State's Electronic Signing Policy, "PKI usage is prescribed only when the "high" level of trust is warranted."

Cost profile of building vs. buying

The researchers evaluated the cost of implementing digital signature capability requiring a Public Key Infrastructure (PKI) system. The analysis included major cost factors for in-house development and third-party development including costs associated with development resources, software licensing, new hardware, consulting resources, ongoing maintenance, and administrative costs. The conclusion is that, considering a three year cost schedule, it would be far more advantageous to leverage a third party solution than to develop in-house capabilities.

In-House Development:	$1,091,600
Third-Party Solution:	$ 558,405

Conclusions

The research suggests four conclusions. (1) Electronic and digital signatures are a legally enforceable method of conducting business, commerce and government affairs. Their use in private commerce and government business will continue to increase. (2) ADOT must evaluate the level of risk for candidate transactions using the State of Arizona, Policy Authority, Office of Secretary of State Electronic Signing Policy to ensure the appropriate level of security is provided. Only transactions deemed to require a "high" level of trust will require the deployment of full digital signature technology. (3) All transactions presented to the research team fit into the "low" or "moderate" transaction risk profile and thus do not require a full deployment of digital signature technology (e.g. a full Public Key Infrastructure System). (4) If ADOT determines a transaction meets the definition of a "high" risk profile, leveraging an external third-party application is clearly our recommended implementation method over building an in-house solution. The department already uses the Adobe LiveCycle product which can be integrated with PKI technology.

The full report: *SPR 534 – Digital Signature Feasibility Study* by Chris Cioffi and Rob Fallows, Principle Consultants of Arrowhead Solutions, Inc, 16841 N. 31st Avenue, Suite 141, Phoenix, AZ (Arizona Department of Transportation, report number FHWA-AZ-08-534, published June 2008) is available on the Internet. Educational and governmental agencies may order print copies from the Arizona Transportation Research Center, 206 S. 17 Ave., MD 075R, Phoenix, AZ 85007; FAX 602-712-3400. Businesses may order copies through ADOT's Engineering Records Section